المحور السادس: مخاطر تقنيات الاتصال الحديثة والأمن الالكتروني

يمثل أمن المعلومات حماية وتأمين الموارد المستخدمة كافة والعمل على سريتها وسلامتها، وفي غياب أمن المعلومات، أو نقصه، أو توقفه وعدم الاستفادة القصوى منه يؤدي إلى فقدان الثقة مما يجعله عبئا على الشركة وعلى هذا الأساس يجب حماية الشركة والمعلومات من الأضرار التي قد تؤدي إلى فشل الأداء وتعود بالخسارة على الشركة والعاملين فيها.

1-مخاطر استخدام تكنولوجيا المعلومات والاتصال: ومن هذا المنطلق يمكن تصنيف مخاطر استخدام تكنولوجيا المعلومات من حيث المصدر إلى (الدلاهمة، 2013، ص17):

أ-مخاطر داخلية: المصدر الرئيس للمخاطر الداخلية يتمثل في موظفي المؤسسة؛ لأنهم الأكثر دراية ومعرفة بنقاط الضعف في نظام الرقابة الداخلي ، ولما لهم من صلاحيات في الدخول إلى النظام حيث ساعد الاستخدام الواسع لتكنولوجيا المعلومات في زيادة المخاطر، ويؤثر هذا النوع من المخاطر على مراحل عمل النظام المختلفة (مرحلة إدخال البيانات، ومرحلة معالجة البيانات، ومرحلة مخرجات النظام)

ب- مخاطر خارجية: تمثل الكوارث الطبيعية و

قراصنة المعلومات أهم مصادر المخاطر الخارجية وتتمثل هذه المخاطر في:

- الفيروسات.
- قراصنة المعلومات.
- التطور التكنولوجي.

1-1-مخاطر الفيروسات على المؤسسات:

من أخطر ما يواجه الشبكات المعلوماتية للمؤسسات إمكانية تدمير ما بها من بيانات أو إتلافها أو تعطيلها عن العمل، وذلك من خلال الفيروس المعلوماتي، وما ساعد في ظهوره وانتشاره ثورة الاتصالات الالكترونية الهائلة، فأصبحت وسائل الاتصال من وسائل انتقال الفيروس إلى مسافات بعيدة جدا من خلال شبكة الانترنيت، فيمكن للمشترك فيها استخدامها في نقل الفيروس إلى أبعد مكان في العالم .

1-1-1-تعريف الفيروس المعلوماتي:

الفيروس المعلوماتي هو عبارة عن برنامج، يقوم بنسخ نفسه على أجهزة الكمبيوتر، وله القدرة على ربط نفسه بالبرامج الأخرى، وكذا إعادة إنشاء نفسه حتى يبدو أنه يتوالد ذاتيا، ويقوم بالانتشار بين برامج الحاسب الآلي المختلفة وبين مواقع مختلفة في الذاكرة .وعند نشاطه يقوم بتدمير البرامج والبيانات المسجلة والمخزنة داخل الحاسب، كما يسبب فشل البرامج وعرض رسائل مزعجة مع تخفيض أداء النظام، وقد يصل الأمر إلى تدمير كل ملفات القرص الصلب المصاب (العاني، 2007، ص119).

توجد من الفيروسات التي تقوم بالتقاط البريد الالكتروني وتقوم بتأليف وإرسال رسائل مرفقة بملحقات ملوثة .وقد ساهم البريد الالكتروني في انتشار الفيروس المعلوماتي بدرجة كبيرة، لأنه يمكن من إرسال رسائل إلى آلاف المستخدمين الذي يشتركون في نظم الحاسب.

1-1-2-خصائص الفيروس المعلوماتي:

تظهر خطورة الفيروس المعلوماتي من خلال خصائصه الضارة المميزة له وتتمثل في (العاني، 2007، ص120):

-القدرة على الاختفاء :حيث تكون للفيروس المعلوماتي القدرة على الاختفاء والتمويه، ويستخدم في ذلك عدة وسائل، كأن يرتبط ببرامج شائعة الاستخدام ومجرد نسخها يجعله ينتقل إلى القرص، وهناك فيروسات تدخل إلى الحاسب في شكل ملفات مختفية لا تظهر عند استعراض فهرس الملفات، ومنها ما تستقر في أماكن مثل الذاكرة التي يصعب ملاحظتها فيها.

-القدرة على الانتشار والاختراق :ساعد تقدم شبكة الاتصالات الحديثة انتشار الفيروس بين ملايين الأجهزة، وساعد في ذلك أيضا سرقة البرامج وتطعيمها بالفيروس وإعادة بيعها، والأكثر من هذا وذاك هو انتشاره في ثوان معدودة من مكان لآخر من العالم، وانتشاره السريع داخل الكمبيوتر نفسه من خلال عمل نسخ عديدة في بضع ثوان.

-القدرة على التدمير :يتمثل نشاط الفيروس التدميري في قيامه بمسح البيانات المخزنة على وسائط أي مسح البيانات وتحويلها إلى الصفر، لذا يسمى بالقنبلة الموقوتة، ويظهر ضرر الفيروس المعلوماتي على البرامج كبيرا جدا، ويلحق الضرر كذلك بأجهزة الحاسب الآلي ولكن بصورة بسيطة.

1-2-القرصنة الالكترونية ومخاطرها على المؤسسات:

من الأسباب القوية لتخوف المؤسسات من استخدام تقنيات الاتصال الحديثة هي المخاطر التي تهدد أمنها، الناتجة أساسا عن التعامل عبر الشبكات المفتوحة خاصة الانترنيت التي ظهر معها ابتكارات في الأساليب الالكترونية للقرصنة.

ويعرف الاختراق الالكتروني بأنه القدرة على الوصول لجهاز أو شبكة أو موقع بطريقة غير مشروعة عن طريق الثغرات الأمنية الموجودة في نظام الحماية الخاص بالهدف، كالدخول على أجهزة الآخرين عنوة أو التلصص داخل شبكاتهم. حيث يتاح للشخص المخترق أن ينقل أو يمسح أو يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين (درار، 2017، ص117).

-المخاطر الناتجة عن القرصنة الالكترونية:

على الرغم من الفوائد والمزايا التي تحققها تقنيات الاتصال الحديثة للمنشآت والدول على حد سواء، لا يزال يهدد تلك التقنيات مخاطر متعلقة بمدى توفر خصوصية البيانات والمعلومات الخاصة بالمتعاملين، لاسيما الانترنيت فيما يلي (العاني، 2007، ص ص117، 118):

-تغيير محتويات معلومات المنشأة على شبكة الاتصال الالكتروني :

-استخدام البيانات على شبكة الاتصال الإلكتروني لتنفيذ بعض الأعمال غير المشروعة:

-التعرف على النظم والسياسات الداخلية للمؤسسة :

-توقف مقر معلومات المنشأة على الشبكة الالكتروني عن العمل :

-تخريب مقر معلومات المؤسسة على الشبكة

2-الأمن الالكتروني في المؤسسات:

إن استخدام اصطلاح أمن المعلومات وان كان استخداما قديما سابقا لوجود وسائل تكنولوجيا المعلومات، الا انه وجد استخدامه الشائع بل والفعلي مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات- وتحديدا الإنترنت – احتلت ابحاث ودراسات أمن المعلومات مساحة كبيرة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة.

– مفهوم أمن المعلومات: لقد اختلفت المفاهيم التي أوردها الباحثون بشأن تحديد مفهوم لأمن المعلومات وفيما يأتي بعض هذه المفاهيم:

-تعريف أمن المعلومات: هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية ، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها والأجهزة ووسائط المعلومات التي تحتوي على بيانات المنشأة، وذلك في جميع مراحل تواجد المعلومة (التخزين، النقل، المعالجة) (الحمادي، 2010، ص14).

-وهناك تعريف آخر للأمن الالكتروني وهو عبارة السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال إلكترونيا عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والزبائن والمنظمين والمستفيدين وأي شخص آخر ممكن أن يكون معرضاً لمخاطر الاختراق (الحمادي، 2010، ص13).

– وسائل تحقيق أمن المعلومات:

هي مجموعة الآليات والإجراءات والأدوات التي تستخدم للوقاية من المخاطر أو تقليل الخسائر بعد وقوع الحدث على المعلومات وأنظمتها. وتتعدد وسائل الحماية من حيث الطبيعة والغرض وفيما يلي بعض هذه الآليات:

–سلامة المعلومات: لكي نحقق الأمن والسرية لمعلومات الشركة يجب أن نضع بعض السياسات والإجراءات التي تستوجب لتوفير الحماية الكافية للمعلومات لعدم الاطلاع عليها من قبل الآخرين غير المصرح لهم .ومن الإجراءات مثلا عمل نسخ احتياطية لبعض الملفات المهمة خشية من التدمير، أو الفقدان وكذلك تطبيق وسائل حماية إضافية مثل مفتش الكابلات، ومحلل البروتوكول الذي يستخدم لفحص محتوى الرزم المعلوماتية التي تنقل عبر شبكة اتصالات نظم

المعلومات. كما إن من متطلبات امن المعلومات وضع عددا من القوانين واللوائح والتوجيهات وعلى مستوى المسؤولية عن امن المعلومات لتحديد الأدوار الرئيسة والحد الأدنى لضوابط أمن المعلومات.

-**التوقيع الالكتروني**: التوقيع الالكتروني يتمثل في حروف و ارقام و اشارات مجموعة في ملف رقمي صغير يساعد على تمييز هوية الموقع وشخصيته دون غيره وبانه هو من قام بإجراء المعاملة و تنفيذها (بوعقل وآخرون، 2016، ص 384).

-تشفير البيانات: التشفير هو عملية دمج المعلومات في شفرة سرية غير مفهومة ثم فك هذه الشفرة بعد وصولها الى وحدة خدمة الويب الامنة ، أي ان التشفير هو استبدال مستند او رسالة باستخدام برنامج معين، و لهذا تنطوي عملية التشفير على تحويل النصوص البسيطة الى رموز (حروف، ارقام، اشارات) قبل ارسالها الى مستقبلها شريطة ان يكون لهذا الاخير القدرة على حل الشفرة و تحويل الرسالة الى صيغتها الاصلية باستخدام مفتاح التشفير (بوعقل وآخرون، 2016، ص 383).

-**مضادات الفيروسات**: وهي مجموعة من البرامج التي تتصدى للفيروسات الداخلة إلى الجهاز وتتفاوت مضادات، من حيث القوة والفاعلية إلا انه يمكن لصناع الفيروسات وناشريها تجاوز مفعولها في كثير من الأحيان (الحمادي، 2010، ص ص 26، 27).

-الجدران النارية: الجدار الناري أو كما يعرف أيضا حائط المنع عبارة عن نظام الكتروني حمائي يعمل بمثابة حاجز ما بين الشبكة الداخلية للمؤسسة وشبكة الانترنيت، ويقوم بترشيح عملية النفاذ ويقننها في حال الدخول إلى مقر معلومات المؤسسة أو الخروج منها، وفقا لقواعد ومبادئ محكمة تحددها المؤسسة صاحبة الشبكة الالكترونية، وهو بذلك يوفر سياسات أمنية للمتعاملين (العاني، 2007، ص134).

قد انتقلت وسائل حماية الشبكات من مستويات الحماية الفردية أو ذات الاتجاه الفردي، التي تقوم على وضع وسائل الحماية ومنها الجدران النارية في المنطقة التي تفصل الشبكة الخاصة عن الموجهات التي تنقل الاتصال إلى الشبكة العالمية (الإنترنت) ، إلى مستويات الأمن المتعددة والتي تقوم على فكرة توفير خطوط إضافية من الدفاع بالنسبة لنوع معين من المعلومات أو نظم المعلومات داخل الشبكة الخاصة ، وتعتمد وسائل الأمن متعددة الاتجاهات والأغراض آليات مختلفة لتوفير الأمن الشامل.